REMARKS

This application has been carefully considered in connection with the Examiner's Final Office Action dated March 31, 2009. Reconsideration and allowance are respectfully requested in view of the following.

Summary of Rejections

Claims 22-35 were rejected under 35 USC § 103.

With regard to the art rejections, the Office Action has cited Sampson et al., U.S. Patent 6,529,624 ("Sampson"); Blakely, III et al., U.S. Patent 5,832,311 ("Blakely"); and Mehring et al., U.S. Patent 6,609,115 ("Mehring").

Summary of Amendments

Claims 22, 25, and 27 are currently amended herein.

Claims 23, 24, 26, and 28-34 were previously presented.

Claims 16-18 and 35 are canceled herein.

Claims 1-15 and 19-21 were previously canceled.

Claims 22-34 are currently pending following this response.

Remarks and Arguments are provided below.

Applicant Initiated Interview

Applicants thank Examiner Cristina Sherr for her time and consideration of the amendments discussed in numerous telephone interviews, culminating in an agreement of claim amendments that will place the application in condition for allowance in the

telephone interview on May 11, 2011. Applicants contacted the Examiner based on the statement made on page 10 of the Examiner's Answer stating, "Note, that were the limitations above-described in claim 22 positively recited, which would also alleviate any issues of 'abstractness', the claim would likely be allowable." The claims have been amended herein as discussed with Examiner Sherr.

Detailed Response

Rejection of Claim 22 Under 35 U.S.C. § 103 (a)

Claim 22 was rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakely

I. Sampson in view of Blakley does not teach or suggest capturing the password provided to the source user authenticator, monitoring the source user authenticator for an approval response and populating the target datastore with the captured password upon receipt of an approval response.

Sampson in view of Blakley does not teach or suggest capturing the password provided to the source user authenticator, monitoring the source user authenticator for an approval response and populating the target datastore with the captured password upon receipt of an approval response.

Claim 22 of the pending application recites in part:

> prompting, by the source user authenticator, the user for identification and user authentication data;
> receiving, by the source user authenticator, identification and user authentication data from the user;
> monitoring, by a password capture process, the source user authenticator for an approval response;
> detecting, by the password capture process, the approval response from the source user authenticator;

> capturing, by the password capture process, the user authentication data provided to the source user authenticator by the user;
>
> populating, by the password capture process, the target datastore with the captured user authentication data associated with the corresponding identification upon detecting the approval response.

Thus, migrating password data from a source (or first) datastore to a target (or second) datastore according to the method of claim 22 may be accomplished without decrypting the password data stored in the source datastore and copying the decrypted password data to the target datastore. Rather, the interceptor captures the password provided by the user to the source user authenticator in response to prompting by the source user authenticator and waits to see whether the source user authenticator approves the user. If the source user authenticator approves the user's password, then the target user authenticator can populate its own datastore with the captured password knowing that the captured password is authentic. In some cases, the password data may be stored in the source datastore as, for example, a hash or other format that is not subject to being decrypted. However, such a method of storage is no impediment for migrating password data from the source datastore to the target datastore according to the method of claim 22 since no decryption is necessary. The only requirement is that the source user authenticator is still functioning such that it is able to verify that the entered password is authentic.

The Final Office Action acknowledges that Sampson does not teach these elements of claim 22 recited above, but alleges that Blakley does disclose these elements in column 7, lines 17-35. *See*, Final Office Action, pp. 4-5. Blakley, in column 7, lines 17-35, discloses synchronization of passwords between a DCE register and a foreign registry that has been configured into the network after the DCE registry has

been populated with user definitions. Blakley further discloses that the synchronization provides a way for a foreign registry to receive the passwords for selected users without the need to wait for those points in time at which the passwords may be changed. In order to accomplish this, and in contrast to claim 22, Blakley requires that passwords stored in a first datastore be decrypted and then passed as plain text passwords to the second datastore. See, for example, Blakley, column 8, which states that "if the value is identified, the password synchronization server retrieves client W's password from the password repository and decrypts it. Next, in block **450**, the password synchronization server returns client W's password to foreign registry Z." This is a completely different method for transferring password data from one repository to another and is inapplicable to systems in which the password is stored as, for example, a hash, which is an item typically not capable of being decrypted. Specifically, Blakley does not teach capturing the password provided to the source user authenticator, monitoring the source user authenticator for an approval response and populating the target datastore with the captured password upon receipt of an approval response as claimed.

II. Neither Sampson nor Blakley teach or suggest migrating password data from a source datastore to a target datastore.

Claim 22 of the pending application recites in part:

> A method for populating password data to a target datastore associated with a target user authenticator that is in communication with a source user authenticator after migration from the source user authenticator, the source user authenticator associated with a source datastore comprising unencrypted user identification data and user authentication data encrypted with a proprietary encryption algorithm, while also responding to user requests for information, the method comprising:

migrating unencrypted data from the source datastore to the target datastore.

The Final Office Action alleges that Sampson discloses this feature citing column 6, lines 2-5, column 7, lines 30-32, and column 17, lines 1-15. *See*, Final Office Action, p. 4. In column 6, lines 2-5, Sampson discloses that each registry server may execute operations using multiple execution threads in which access of each thread to a registry repository is managed by an access control library. Sampson, in col. 7, lines 30-32, discloses that the registry server has an authentication server module that manages concurrent access of multiple users of browsers to the registry repository. Sampson further discloses, in column 17, lines 1-15, a computer system that includes a main memory for storing temporary variables or other intermediate information during executions of instructions to be executed by a processor, a static storage device for storing static information and instructions for processor, and a storage device for storing information and instructions. Nothing in these passages teach or suggest migrating the source datastore to the target datastore as claimed.

Rather, in contrast to the claims, Sampson is simply directed to a system that controls access to information resources. *See*, Sampson, Abstract. In particular, Sampson discloses a session manager that determines whether the client is involved in an authenticated session with any access server in the system. *See, e.g.,* Sampson, Abstract. If so, the client is permitted to access the resources without logging in to the specific access server that is associated with the protected server. *See, e.g.,* Sampson, Abstract. Thus, Sampson merely teaches a single sign-on system such that a user only has to authenticate themselves once rather than multiple times even though the system may include multiple protected resources requiring authentication. Sampson does not

disclose migrating identification and authentication (e.g., password) data from a source datastore to a target datastore. In fact, Sampson is completely unconcerned with migrating data of any type at all. Sampson is simply concerned with providing a single sign-on for a user so that the user does not have to log in multiple times in order to access various protected resources in the system. Such a system is unrelated to migrating authentication data from one datastore to another without requiring a user to re-enroll.

Blakley does not cure this deficiency in Sampson. Blakley provides password synchronization between a main data store and a plurality of secondary data stores. *See*, *e.g.,* Blakley, Abstract. This enables the user to maintain a single, unique password among the plurality of secondary datastores. Thus, Blakley uses a password synchronization server to store user names and plain-text passwords securely and to respond to requests from secondary datastores for their retrieval. The passwords are sent to the secondary datastores using encryption that is decipherable by the secondary datastores. However, notably absent from Blakley is any teaching or suggestion of migrating data from a source datastore to a target datastore. Note that data migration is not equivalent to data replication. Also, Blakley does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information and without decrypting the data stored in the first vendor's product.

For at least the reasons established above in sections I and II, Applicants respectfully submit that independent claim 22 is not taught or suggested by Sampson in view of Blakely and respectfully request allowance of this claim.

Rejection of Remaining Claims

Claims 25-35 were rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakely.

Claims 23 and 24 were rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakely further in view of Mehring.

Claim 35 has been canceled herein, rendering the rejection of this claim moot. The remaining claims 23-34 all depend on claim 22. Accordingly, Applicants assert that claims 23-34 are in condition for allowance for at least the reasons established above.

Conclusion

Consideration of the foregoing remarks and reconsideration of the application is respectfully requested by Applicants. No new matter is introduced by way of this response. If any fee is due as a result of the filing of this paper, please appropriately charge such fee to Deposit Account Number 21-0765 of Sprint. If a petition for extension of time is necessary in order for this paper to be deemed timely filed, please consider this a petition therefore.

If a telephone conference would facilitate the resolution of any issue or expedite the prosecution of the application, the Examiner is invited to contact the undersigned at the telephone number given below.

Respectfully submitted,

Date: **May 12, 2011**.

/Michael W. Piper/
Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5601 Granite Parkway, Suite 750
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)